

Serial No. **09/934,477**

Docket No. **P-0218**

Amdt. dated June 5, 2006

Reply to Office Action of March 9, 2006

REMARKS

By the present response, Applicant has canceled claim 21 without disclaimer. Further, Applicant has amended claims 1, 20 and 22 to further clarify the invention. Claims 1-20 and 23 remain pending in the present application.

In the Office Action, claim 1 has been objected to because of informalities. Claim 20 has been rejected under 35 U.S.C. § 102(e) as being anticipated over U.S. Patent No. 6,282,193 (Hluchy et al.). Claims 1-2, 8-9, 11-14, 15-18 and 24-27 (sic) have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rigney et al. (RFC 2138) in view of U.S. Patent No. 6,538,996 (West et al.). Claim 11 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over RFC 2138 in view of West et al. and further in view of U.S. Patent No. 6,088,799 (Morgan et al.). Claims 3-7, 10, 19 and 21-23 have been objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Allowable Subject Matter

Applicant thanks the Examiner for indicating that claims 3-7, 10, 19 and 21-23 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Serial No. **09/934,477**

Docket No. **P-0218**

Amdt. dated June 5, 2006

Reply to Office Action of March 9, 2006

Claim Objections

Claim 1 has been objected to because of informalities. Applicant has amended this claim to further clarify the invention and respectfully requests that this objection be withdrawn.

Response to Arguments

The Examiner maintains that Hluchyj discloses authenticating an access-request message prior to performing user authentication of the access-request message, at col. 3, lines 49-57, authentication, and col. 6, lines 1-19, error correction. However, the Examiner appears to misunderstand the terms “authentication” and “error correction”. Authentication, as recited in the claims of the present application, relates to verification that an access-request message is authorized and valid and verifying the identity of a user. In contrast, error correction merely relates to checking whether transmitted data or information has been damaged and correcting the damaged data or information. Error correction has nothing to do with authentication as recited in the claims of present application.

Further, as noted in Applicant’s previously filed response, the cited portions of Hluchyj merely disclose that packet protocol processing includes support for user authentication. This is not authenticating an access-request message prior to performing user authentication of the access-request message such that abnormal access-request messages are not processed for user authentication.

Further, the portions of RFC 2138., page 6 cited by the Examiner do not disclose or suggest processing the access-request message if the access-request message is successfully verified, as recited in the claims of the present application. As noted in Applicant's previously filed response, RFC 2138 merely discloses that after receiving the request, the sending client is validated. This is not processing an access-request message after the message is successfully verified. RFC 2138 does not disclose or suggest message verification or verification of the sending client after a message is verified.

35 U.S.C. § 102 Rejections

Claim 20 has been rejected under 35 U.S.C. § 102(e) as being anticipated by Hluchyj et al. Applicant has amended this claim with the subject matter of claim 21, deemed allowable by the Examiner. Accordingly, Applicant submits that this claim is patentable over the cited reference at least for this reason. Accordingly, Applicant respectfully requests that this rejection be withdrawn and that this claim be allowed.

35 U.S.C. § 103 Rejections

Claims 1, 2, 8, 9, 11-14 and 15-18 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over RFC 2138. in view of West et al. Applicant respectfully traverses these rejections.

West et al. discloses a system that identifies, models, and automates aspects of remote access to a local computer network. The system involves several inter-related components and

provides support for determining an appropriate telephone access number for use by a remote user, and provides support to that user if a connection cannot be successfully established. Difficulties associated with distribution and searching of telephone access number data are overcome, in part, by organizing data that is stored on a remote computer to be both compact and easily searched and by incrementally downloading that data as a background communication task.

Regarding claims 1, 9 and 17, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, *inter alia*, executing an encryption algorithm using the access-request message having the temporary authenticator value and the encrypted user password to generate a message digest, the access-request message having an authenticator field that is filled with a prescribed value, or generating a final access-request message by replacing the value of the authenticator field with the message digest, or transmitting the final access-request message to an authentication, authorization and accounting server, or processing the access-request message if the access-request message is successfully verified, or performing user authentication by decrypting an encrypted user password of the process access-request message using a temporary authenticator value of the processed access-request message and a shared secret key that is known to each of a message transmitter and a message receiver.

The Examiner again asserts that RFC 2138 discloses transmitting the final access-request message to an AAA server on page 6 with the disclosure of receiving the request. However, as noted previously, these portions of RFC 2138 merely disclose that once the RADIUS server receives the request, it validates the sending client. This is not transmitting a final access-request message to an AAA server, the final access-request message being generated using the access-request message and replacing the value of the authenticator field with the message digest, or verifying the access-request message by the AAA server, as recited in the claims of the present application. RFC 2138 merely discloses a request for authentication from a client being received and validation of the sending client. In contrast, the limitations in the claims of the present application relate to transmitting a final access-request message including a message digest, and also verifying the access-request message.

The Examiner admits that RFC 2138 does not disclose or suggest executing an encryption algorithm to generate a message digest and filling in fields of a request message, but asserts that West et al. discloses these limitations at col. 28, lines 25-29. However, these portions merely disclose that in response to receiving N1, delivery a computes a one-way hash function using a secret password and the random challenge, N1, that delivery a then sends the computed hash value to delivery b, and that in order to determine whether delivery a truly knows the secret password P, delivery b would compute the hash value directly if it knew the secret password. This is not using the access-request message having the temporary authenticator value and

encrypted user password to generate a message digest, as recited in the claims of the present application. Further, none of the cited references disclose or suggest the access-request message having an authenticator field that is filled with a prescribed value. The mere disclosure in West et al. of a hash function and MD5 hash function, computing a hash function, or how the hash function is computed, do not disclose or suggest these limitations in the claims of the present application.

Moreover, the Examiner again asserts that RFC 2138 discloses decoding the access-request message if the access-request message is successfully verified on page 6 by the disclosure of validates sending client. However, as noted previously, these portions of RFC 2138 merely disclose that once the RADIUS server receives the request, it validates the sending client. This is not processing the access-request message if the access-request message is successfully verified, as recited in the claims of the present application. These portions of RFC 2138 merely disclose that after receiving the request, the sending client is validated. In contrast, the limitations in the claims of the present application relate to processing the access-request message after the message is successfully verified. Further, none of the cited references disclose or suggest performing user authentication by decrypting an encrypted user password of the processed access-request message using a temporary authenticator value of the processed access-request message and a shared secret key that is known to each of a message transmitter and a message receiver, as recited in the claims of the present application. The Examiner fails to provide any

portion of any cited reference that discloses or suggests these limitations in the claims of the present application.

Regarding claims 2, 8, 11-14, 15, 16 and 18, Applicant submits that these claims are dependent on one of independent claims 1, 9 and 17 and, therefore, are patentable for the same reasons noted previously regarding these independent claims. For example, Applicant submits that none of the cited references disclose or suggest where the prescribed value is a value previously defined between a foreign agent and the AAA server, or where the randomly generated authenticator value is created differently every time a message is generated, or where the temporary authentication value is randomly generated each time a new access-request message is generated such that the temporary authenticator value is not known beforehand.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 1, 2, 8, 9, 11-14 and 15-18 of the present application. Applicant respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 11 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over RFC 2138 in view of West et al. and Morgan et al. Applicant submits that this claim is dependent on independent claim 9 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim.

Serial No. **09/934,477**

Docket No. **P-0218**

Amdt. dated June 5, 2006

Reply to Office Action of March 9, 2006

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose suggest or render obvious the limitations in the combination of the claim 11 of the present application. Applicant respectfully request that this rejection be withdrawn and that this claim be allowed.

Serial No. 09/934,477

Docket No. P-0218

Amdt. dated June 5, 2006

Reply to Office Action of March 9, 2006

CONCLUSION

In view of the foregoing Amendments and remarks, Applicant submits that claims 1-20, 22 and 23 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned attorney, Frederick D. Bailey, at the telephone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
FLESHNER & KIM, LLP



John C. Eisenhart
Registration No. 38,128
Frederick D. Bailey
Registration No. 42,282

P.O. Box 221200
Chantilly, Virginia 20153-1200
(703) 766-3701 JCE/FDB:tlg

Date: June 5, 2006

\\Fk4\Documents\2000\2000-122\89175.doc

Please direct all correspondence to Customer Number 34610